IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Natsume Matsuzaki

Serial No.: 09/544,069

Filed: April 6, 2000

For: MULTI-WORD ARITHMETIC DEVICE FOR FASTER COMPUTATION OF CRYPTOSYSTEM CALCULATIONS

Patent Examiner: Mathhew Smithers

Group Art Unit: 2137

September 17, 2004

Irvine, California 92614

TRANSMITTAL OF PRIORITY DOCUMENT

MAIL STOP AMENDMENT
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed is the certified copy of the priority document Japan 11-099657, for the above-identified patent application in accordance with 35 USC §119.

Please acknowledge receipt of this priority document.

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on September 17, 2004by James Lee

Signature

Date of Signature: September 17, 2004

Very truly yours,

SNELL & WILMER LLP

Julio Loza, Reg. No. 47,758
1920 Main Street, Suite 1200
Irvine, CA 92614
949/253-4924

Matsushita Electric Industrial Co.
Ltd. 09/514,069
32172-9800

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　４月　７日

出願番号
Application Number: 平成１１年特許願第０９９６５７号

出願人
Applicant (s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　３月３１日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０２２９７４

【書類名】　特許願

【整理番号】　2022510153

【提出日】　平成11年 4月 7日

【あて先】　特許庁長官殿

【国際特許分類】　G09C　1/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　松崎　なつめ

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　奥村　康男

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　小野　貴敏

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　多倍長演算装置

【特許請求の範囲】

【請求項１】　複数種類の１ワード演算を処理する演算部と、

前記演算部の入出力データを格納するメモリ部と、

前記演算部の演算の種類と演算ワード数を指定して演算部を制御し、

さらに前記メモリ部のアドレスを指定する制御部からなる多倍長演算装置。

【請求項２】　前記メモリ部から前記演算部に、１ワードの入力データを少なくとも２つ同時に供給することを特徴とする請求項１記載の多倍長演算装置。

【請求項３】　前記請求項２記載の前記メモリ部を少なくとも２つのサブメモリ部に分割し、各サブメモリ部から１ワードずつの入力データを、前記演算部に供給することを特徴とする請求項２記載の多倍長演算装置。

【請求項４】　前記演算部は、乗算器とその出力を累算する加算器を含み、前記演算制御部の制御に応じて、乗算演算、または乗算とその結果の累算演算、または加算演算のいずれかを処理することを特徴とする請求項１記載の多倍長演算装置。

【請求項５】　前記制御部は、前記演算部とメモリ部を用いた所定のシーケンス処理を制御することを特徴とする請求項１記載の多倍長演算装置。

【請求項６】　前記メモリ部に、前記演算部からの入出力データを一時格納し、また前記制御部からのアドレス制御を一時格納する、メモリ入出力部を追加したことを特徴とする請求項１記載の多倍長演算装置。

【請求項７】　前記メモリ入出力部を介して、外部からメモリ部への直接の書き込みと読み出しを可能とすることを特徴とした請求項６記載の多倍長演算装置。

【請求項８】　前記メモリ部に格納されている各nワードの第１の入力A 、第２の入力Bと法Pを入力として、前記演算部でA+B-Pの演算を行い、その結果の桁上げ信号を前記制御部に入力し、前記制御部において前記桁上げ信号が１のときは前記演算部の結果を前記メモリに格納し、０のときに演算部の結果に法Ｐを加算したものを前記メモリに格納するように制御することにより、加算剰余演算を

行うことを特徴とする請求項１記載の多倍長演算装置。

【請求項９】　１ワードをkビット、Rを(k×n+1)ビットの値2^(k×n)としたとき、前記メモリ部に格納されている２ｎワードの入力A、ｎワードの法Pを入力として、Ｐを法とした剰余体におけるA×R^(-1)の値を求めてモンゴメリリダクション演算を行う多倍長演算装置であって、

前記メモリ部に、予めnワードのV=-P^(-1) modRの値を求めて格納しておき、前記演算制御部が、前記演算部で、前記Aの下位nワードと前記Vの部分積を最下位ワードから桁を合わせて順次加算し、下位nワードまでを求めて、その結果を中間値Bとして前記メモリ部に格納する第１の乗算制御と、

前記中間値Bと前記法Ｐの部分積を最下位ワードを０ワード目としたとき、n-2ワード目から桁を合わせて順次加算し２ｎ-1ワード目までを求めて、その結果の上位n+1ワードを中間値Cとして前記メモリ部に格納する第２の乗算制御と、

前記Aの上位n+1ワードを中間値Dとして、

前記中間値Cと中間値Dの最下位ワードを加算したときの１ビットの桁上げ信号と、加算結果の１ワードがゼロでないときに１がセットされ、ゼロのときに０がセットされる１ビットのノンゼロ信号を出力する信号生成部と、

前記中間値Cと中間値Dの上位nワード、および前記各１ビットの桁上げ信号とノンゼロ信号を加算する加算制御と、

前記加算結果が前記法Ｐより大きい場合に、Ｐ以下になるまで前記加算結果よりＰを減算する減算制御を備え、

前記減算結果をモンゴメリリダクションの結果として前記メモリ部に格納することを特徴とした請求項１記載の多倍長演算装置。

【請求項１０】　前記信号生成部と加算制御部が、前記演算部において、前記各n+1ワードの中間値Cと中間値Ｄに１ワードのオール１の値（2^k）-1を加算して、加算結果の上位nワードを出力することを特徴とする請求項９記載の多倍長演算装置。

【請求項１１】　前記加算制御と減算制御を、請求項８記載の加算剰余演算制御により実現する請求項９記載の多倍長演算装置。

【請求項１２】　前記第１、第２の乗算制御は、その出力部分積のmワード目

は、ｎワードの第１の被乗数のiワード目と第２の被乗数のjワード目を、i+j=mを満たすようにすべての組み合わせで選んで、それぞれを前記演算部に入力して結果を累算することを特徴とした請求項９記載の多倍長演算装置。

【請求項１３】　前記出力部分積のmワード目の最終の累積結果を前記メモリに格納するのと同時に、前記累算結果の上位にあふれた値を初期値とした、m+1ワード目の累算に対応した被乗数の前記メモリ部から前記演算部への読み出しを行うことを特徴とした請求項１２記載の多倍長演算装置。

【請求項１４】　前記第１の被乗数のiワード目と第２の被乗数のjワード目をメモリから前記演算部に呼び出して部分積を求めるのと同時に、出力部分積のmワード目の部分累算結果を前記メモリから呼び出して、前記部分積と桁を合わせて加算し、同時に加算結果を対応する桁のメモリ部に格納することを特徴とした請求項１２記載の多倍長演算装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号演算などに用いられる多倍長の剰余演算装置に関し、特に楕円曲線暗号のように種々の演算を決められたシーケンスで行う場合に適している。

【０００２】

【従来の技術】

従来、RSA暗号の演算装置として、乗算器とメモリからなる専用の演算装置が製品化されている。これは長語長のべき乗剰余演算処理だけを対象として、短いビット幅の乗算器を繰り返し用いて実現するものであり、CPUと組み合わせてコプロセッサとして用いる。

【０００３】

これに対し、近年RSA暗号の次の公開鍵暗号として注目を集めているのが楕円曲線暗号である。この暗号方式は、RSA暗号では可能であった強力な攻撃法（Index Calculus法）が通用しないことにより、RSA暗号に比べ非常に短い鍵データ長であっても十分な安全性が確保できる。RSA暗号が1024ビット鍵で達成できる安全性を、楕円曲線暗号では160ビット鍵で確保する。しかし、一方、楕円曲線暗

号ではRSA暗号が基本的にべき乗剰余演算だけであったのに対し、四則演算他種々の演算が必要となり、またあらかじめ決まってはいるが条件分岐を含む複雑な手順での演算が必要になる。この楕円曲線暗号を従来のRSA暗号専用のコプロセッサを用いると、コプロセッサの演算はわずかとなり、ほとんどがCPUを用いた演算になってしまい、CPUとコプロセッサの制御の行き来によるオーバヘッドが大きくなり高速処理が実現できない。

【０００４】

また、全部をCPUソフトで実現すると、実装されるメモリの制限上、演算部に効率的にデータが供給できず、高速処理が実現できない。

【０００５】

【発明が解決しようとする課題】

そのため、本発明では、楕円曲線処理に必要となる種々の演算を、共通の演算部を兼用してこれを絶え間なく動作するようにメモリ部からデータを供給する。これにより回路規模を抑えながら楕円曲線暗号処理に必要となる、種々の多倍長演算を効率的に実施することを目的とする。

【０００６】

また、１つの演算部を繰り返し用いて多倍長の演算を行うため、演算幅の増減に柔軟に対応できる。繰り返し回数を増加することにより、ハード変更なしで安全性を高めることができる。

【０００７】

【課題を解決するための手段】

本発明の第１の構成における多倍長演算装置は、

複数種類の1ワード演算を処理する演算部と、

前記演算部の入出力データを格納するメモリ部と、

前記演算部の演算の種類と演算ワード数を指定して演算部を制御し、さらに前記メモリ部のアドレスを指定する制御部からなることを特徴とする。

【０００８】

本発明の第２の構成における多倍長演算装置は、第１の構成における前記メモリ部から前記演算部に、１ワードの入力データを少なくとも２つ同時に供給する

ことを特徴とする。

【０００９】

本発明の第３の構成における多倍長演算装置は、第２の構成における前記メモリ部を少なくとも２つのサブメモリ部に分割し、各サブメモリ部から1ワードずつの入力データを、前記演算部に供給することを特徴とする。

【００１０】

本発明の第４の構成における多倍長演算装置は、第１の構成における、

前記演算部が、乗算器とその出力を累算する加算器を含み、前記演算制御部の制御に応じて、乗算演算、または乗算とその結果の累算演算、または加算演算のいずれかを処理することを特徴とする。

【００１１】

本発明の第５の構成における多倍長演算装置は、第１の構成における、

前記制御部が、前記演算部とメモリ部を用いた所定のシーケンス処理を制御することを特徴とする。

【００１２】

本発明の第６の構成における多倍長演算装置は、第１の構成における、

前記メモリ部に、前記演算部からの入出力データを一時格納し、また前記制御部からのアドレス制御を一時格納する、メモリ入出力部を追加したことを特徴とする。

【００１３】

本発明の第７の構成における多倍長演算装置は、第６の構成における、

前記メモリ入出力部を介して、外部からメモリ部への直接の書き込みと読み出しを可能とすることを特徴とする。

【００１４】

本発明の第８の構成における多倍長演算装置は、第１の構成における、

前記メモリ部に格納されている各nワードの第１の入力A 、第２の入力Bと法Pを入力として、前記演算部でA+B-Pの演算を行い、その結果の桁上げ信号を前記制御部に入力し、前記制御部において前記桁上げ信号が1のときは前記演算部の結果を前記メモリに格納し、0のときに演算部の結果に法Ｐを加算したものを前

記メモリに格納するように制御することにより、加算剰余演算を行うことを特徴とする。

【００１５】

本発明の第９の構成における多倍長演算装置は、第１の構成において、

1ワードをkビット、Rを(k×n+1)ビットの値$2^{(k\times n)}$としたとき、前記メモリ部に格納されている２ｎワードの入力A、ｎワードの法Pを入力として、Ｐを法とした剰余体における$A\times R^{(-1)}$の値を求めてモンゴメリリダクション演算を行う多倍長演算装置であって、

前記メモリ部に、予めnワードの$V=-P^{(-1)} \bmod R$の値を求めて格納しておき、前記演算制御部が、

前記演算部で、前記Aの下位nワードと前記Vの部分積を最下位ワードから桁を合わせて順次加算し、下位nワードまでを求めて、その結果を中間値Bとして前記メモリ部に格納する第１の乗算制御と、

前記中間値Bと前記法Ｐの部分積を最下位ワードを０ワード目としたとき、 n-2ワード目から桁を合わせて順次加算し２ｎ-1ワード目までを求めて、その結果の上位n+1ワードを中間値Cとして前記メモリ部に格納する第２の乗算制御と、

前記Aの上位n+1ワードを中間値Dとして、

前記中間値Cと中間値Dの最下位ワードを加算したときの１ビットの桁上げ信号と、加算結果の1ワードがゼロでないときに１がセットされ、ゼロのときに０がセットされる1ビットのノンゼロ信号を出力する信号生成部と、

前記中間値Cと中間値Dの上位nワード、および前記各1ビットの桁上げ信号とノンゼロ信号を加算する加算制御と、

前記加算結果が前記法Ｐより大きい場合に、Ｐ以下になるまで前記加算結果よりＰを減算する減算制御を備え、

前記減算結果をモンゴメリリダクションの結果として前記メモリ部に格納することを特徴とする。

【００１６】

本発明の第１０の構成における多倍長演算装置は、第9の構成における、

前記信号生成部と加算制御部が、前記演算部において、前記各n+1ワードの中

間値Cと中間値Dに1ワードのオール１の値（2^k）-1を加算して、加算結果の上位nワードを出力することを特徴とする。

【００１７】

本発明の第１１の構成における多倍長演算装置は、第９の構成における、

前記加算制御と減算制御を、請求項８記載の加算剰余演算制御により実現する。

【００１８】

本発明の第１２の構成における多倍長演算装置は、第９の構成における、

前記第１、第２の乗算制御は、その出力部分積のmワード目は、ｎワードの第１の被乗数のiワード目と第２の被乗数のjワード目を、i+j=mを満たすようにすべての組み合わせで選んで、それぞれを前記演算部に入力して結果を累算することを特徴とする。

【００１９】

本発明の第１３の構成における多倍長演算装置は、第１２の構成における、

前記出力部分積のmワード目の最終の累積結果を前記メモリに格納するのと同時に、前記累算結果の上位にあふれた値を初期値とした、m+1ワード目の累算に対応した被乗数の前記メモリ部から前記演算部への読み出しを行うことを特徴とする。

【００２０】

本発明の第１4の構成における多倍長演算装置は、第１２の構成における、

前記第１の被乗数のiワード目と第２の被乗数のjワード目をメモリから前記演算部に呼び出して部分積を求めるのと同時に、出力部分積のmワード目の部分累算結果を前記メモリから呼び出して、前記部分積と桁を合わせて加算し、同時に加算結果を対応する桁のメモリ部に格納することを特徴とする。

【００２１】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて説明する。

【００２２】

まず、一例として楕円曲線暗号の演算などに用いられる加算剰余演算の場合で

本発明を説明する。図１に多倍長演算装置の構成を示す。１は1ワードの演算部、２は加算剰余演算の対象となるデータを格納するメモリ部である。ここで1ワードとは処理の単位となるビット長であり、一般には16ビットや32ビットとなる。メモリ部は２つのサブメモリ部３と４に分かれており、それぞれ1タイミングに２つの1ワードデータを書き込み、または読み出しできるものとする。５は演算部やメモリ部の入出力を一時蓄えるためのメモリ入出力部である。メモリ入出力部を介して、外部よりメモリ部へデータの入出力も行う。また６は演算部を制御し、またメモリ入出力部にアドレスを供給する制御部である。

【００２３】

図２に演算部の構成例を示す。１０は３入力加算器、１１は結果を蓄えるレジスタ（Reg）である。演算部には３つのそれぞれ1ワードのデータが同時に入力され、また同時にレジスタ１１に蓄えられている前タイミングでの演算結果が出力される。

【００２４】

以下では、この多倍長演算装置を用いて５ワードの加算剰余演算を行う際の手順を説明する。5ワードの値を、例えばA=(a4，a3，a2，a1，a0)のように表す。a4,...,a0はそれぞれ1ワードで、a4が最上位、a0が最下位の1ワードとする。２つの入力をA=(a4，a3，a2，a1，a0)、B=(b4，b3，b2，b1，b0)とし、法をP=(p4，p3，p2，p1，p0)としたとき、加算剰余演算は、C=(c4，c3，c2，c1，c0) = A + B mod Pを求めるものとする。ここで、modPはPで除したときの剰余を示す。

【００２５】

図３にメモリ１およびメモリ２のメモリマップを示す。メモリ１には入力のAとP、メモリ２には入力Ｂと出力Cおよび、ワーク領域Wが配置される。それぞれ最下位ワードから順に格納される。入力データA、B、Pの格納は図１におけるメモリ入出力部を介して外部から行うとよい。また出力Ｃについてもメモリ入出力部を介して外部に読み出すとよい。なお、ここでの外部とは例えばホストCPUの内部メモリとする。

【００２６】

このメモリを用いた加算剰余演算の処理手順を図４に示す。まず、図２に示す

Reg１１およびCarry入力を０に設定して、メモリ１から入力Aの最下位a0、メモリ２から入力BとPの最下位b0、 p0をそれぞれ同時に演算部に入力する。そして、図２に示す３入力加算器で、a0+b0-p0の演算を行い、結果をReg１１に格納する。次に、次の桁のa1、 b1、 p1をメモリから獲得して前の桁のキャリーを含めた加算演算をするのと同時にRegに格納されている前の桁の結果をメモリ２のw0に格納する。メモリ１からはa1、p1の読み出し、メモリ２からはb1の読み出しと、w0の書き込みが1タイミングに同時に行われる。なお、各メモリは１タイミングに２つのデータをアクセスできるものとしている。

【００２７】

以降同様にして、W=A+B-Pの演算を行う。この結果、桁上げ信号carryが０になったときは（図４における左側のルート）、A+Bの結果がＰ未満であったことを示すため、結果にＰを加えて引き戻す。桁上げ信号は演算部から制御部に通知されて、制御部において分岐を伴ったシーケンス制御がなされる。ＷとＰの加算演算は、メモリ１の法Ｐとメモリ２のW領域の最下位ワードから１ワードずつ演算器に入力し、１つ前の結果をメモリ２のＣに同時に格納することにより実施する。メモリ１は同時に１回だけアクセス、メモリ2は読み出しと書き込みの計２回アクセスする。また、桁上げ信号carryが１のときは（図４における右側のルート）、Wの結果をそのまま出力の領域Ｃに格納する。この場合はメモリ２のみを読み出しと書き込みの計２回アクセスする。

【００２８】

また、別の例としてモンゴメリ方式を実現する本発明の説明する。モンゴメリ方法は、暗号演算で多用される剰余演算を高速に行う方法である。詳細は例えば、岡本龍明・太田和夫共編「暗号・ゼロ知識証明・数論」共立出版、１９９５年、を参考にすることにし、ここでは演算の概要だけを説明する。以下は、P＜R=2m とし、Ｐ２程度の大きさのＡに対して、Ｍ＝Ａ・Ｒ－１ modPを求める、モンゴメリリダクションと呼ばれている処理である。

【００２９】

入力：Ａ（２ｍビット程度の値）

前計算：Ｖ＝－Ｐ－１ modR

出力：Ｍ＝Ａ・Ｒ－１ modP

処理：

step1: B=A×V modR

step2: M=(B×P + A) / R

step3: M modPを出力

図１の多倍長演算装置の構成を用いる。図５にモンゴメリ演算の場合の演算部の構成を示す。この演算部は、1ワード幅の乗算器を備え、乗算結果を加算器で累算する。制御により加算器としても用いることができ、先に述べた例の加算剰余演算も実現できる。

【００３０】

以下では、上記step1-3の各処理の実現について順次説明する。なお、以下の説明では、P、 Vがそれぞれ5ワード、Ａが１０ワードの場合について説明する。

【００３１】

[step1]

Aの下位５ワードとVの積を桁を合わせて最下位から累算し、下位5ワードまで求める。modRをとっているために、それより上位は求める必要がない。例えば、メモリ1に格納したAの下位５ワード=(a4，a3，a2，a1，a0)と、メモリ２に格納したV=(v4，v3，v2，v1，v0）を乗算して、メモリ1のＢ領域に格納する場合について説明する。図６では、5ワードのAとVの積を筆算の要領で部分積を桁を合わせて累積することにより求める様子を示している。

【００３２】

(1) まず、a0とv0を同時に２つのメモリから読み出して、図５の乗算器に入力する。結果の下位1ワード分をメモリ１のb0に格納し、それより上位は1ワード分シフトダウンして、加算器の一番右の入力に設定する。

【００３３】

(2) 次に、a1とv0を同時に２つのメモリから読み出して、乗算して結果を加算器で累算する。なお、このメモリ読み出しと(1)におけるb0の格納を同時に行うと、処理時間が削減できる。またa0とv1を乗算して結果を加算器で累算する。なお、この２つの部分積は桁が一致しており、２つの被乗数の添え字の数字を加算

すると１になる。これらの結果の下位1ワード分をメモリ１のb1に格納し、それより上位は1ワード分シフトダウンして、加算器の一番右の入力に設定する。

【００３４】

(3) 次に、桁が一致している、a2とv0の乗算と累算、a1とv1の乗算と累算、a0とv2の乗算と累算を行う。なお、このメモリ読み出しと(2)におけるb1の格納を同時に行うと、処理時間が削減できる。また、この桁では、２つの被乗数の添え字の数字を加算すると２になる。累算の結果の下位1ワード分をb2に格納し、それより上位は1ワード分シフトダウンして、加算器の一番右の入力に設定する。

【００３５】

以下同様に作業を続ける。なお、この例では、下位mビットは5ワード分となる。そのため、２つの被乗数の添え字の数字の和が４になる桁までを求めればよい。結果をB=(b4，b3，b2，b1，b0)とする。なお、最後に演算部のレジスタに残った、5ワードより上位の値は切り捨てる。

【００３６】

[step2]

Ｂ×Ｐの演算も、step1と同様に部分積を累算する方法で行う。ただし、この場合はＡとの加算も行い、その結果の上位mビットが必要になる。step1の場合と同様に、Ｂ、Ｐが5ワード、Ａが１０ワードの場合で手順を説明する。図７では、筆算の要領で部分積を桁を合わせながら累積する様子を示している。

【００３７】

まず、ＢとＰの被乗数の添え字の和が３となる桁から部分積を求め、最後のb4*v4の桁までの積を桁をそろえて累算する。累算結果のうち最下位ワードを除いた6ワード分をＣとする。またＡのうち、このＣと桁を合わせた上位６ワードをＤとする。

【００３８】

ＣとＤの最下位ワード（図７においてハッチング）に着目し、これらを加算したときの1ビットの桁上げ信号を求める。また、加算結果の1ワードがゼロでないときに１がセットされ、ゼロのときに０がセットされる、ノンゼロ信号も求める。そして、ＣとＤの最下位ワードを除いた各5ワード、および前記桁上げ信号と

ノンゼロ信号の和を求め、これを出力Mとする。つまり、前記桁上げ信号とノンゼロ信号により、CとDの最下位ワードを除いた各5ワードの和に、

・桁上げ信号＝０、ノンゼロ信号＝０のとき、０

・桁上げ信号＝０、ノンゼロ信号＝１のとき、１

・桁上げ信号＝１、ノンゼロ信号＝０のとき、１

・桁上げ信号＝１、ノンゼロ信号＝１のとき、２

が加算され、出力Mとなる。

【００３９】

勿論この加算についても演算部内の1ワード幅の加算器を繰り返し用いるものとする。

【００４０】

なお、上位mビットの出力Mを、部分積を最下位から全部順番に求めず、n-2ワード目より上位だけを用いて求めている。そのため、高速化が実現できている。

【００４１】

なお、上記桁上げ信号とノンゼロ信号を生成してから出力Mを求める代わりに次のようにしてMを求めることも出来る。

【００４２】

前記6ワードのCとDと、その最下位ワードの位置に1ワードの各ビットに１をセットした値（オール１と呼ぶことにする）を加算する。そして、その結果の上位５ワードをMとする。この方法では、桁上げ信号やノンゼロ信号を生成する部分を設けなくても、図５で示した演算器を利用することにより実現できるため、回路規模の面より有利である。

【００４３】

以上の処理により、BとPの部分積のうち例えばb0*p0、 b1*p0などの添え字の和が２以下の部分積は求めなくてもよく、処理速度の高速化が実現できる。また、桁が変わる毎にその桁の結果をメモリに格納するが、この格納と次の桁の読み出しを同時に処理するために、演算部は休みなく動作することができる。

【００４４】

[step3]

Ｍの値を法Ｐ以下になるまでＰを減算する。この減算についても演算部内の1ワード幅の加算器を繰り返し用いて、その最上位ワードからのキャリー出力により、Ｐ以下になることを確認する。

【００４５】

なお、以上の説明ではmビットを５ワードとしたが、これに限定されるものではない。例えば楕円曲線暗号で用いる場合にはmは160程度、RSA暗号の場合には1024程度になる。

【００４６】

また、図１における構成では演算部とメモリ部のタイミングを取るため、および外部からメモリ部に直接アクセスするために、メモリ入出力部を設けたが、必要のない実装もある。

【００４７】

また、図１における構成ではメモリ１、２がそれぞれ独立のメモリであり、１タイミングに２回アクセスできるようなものとしたが、これを実現するためメモリ部だけに２倍の周波数のクロックを与えるとしてもよい。またデュアルポートメモリを用いてもよい。

【００４８】

【発明の効果】

以上のように本発明によれば、楕円曲線暗号に必要となる種々の多倍長演算を、小さなハードで高速に処理できる。また繰り返し回数を制御するだけで、ハード自身は変更することなく安全性を向上することができる。またメモリ部をうまく配置実現することにより、演算部を休みなく動作させて、処理の高速化が実現できる。

【００４９】

また、本発明の多倍長演算装置を用いて、楕円曲線暗号で必要となる加算剰余演算と、モンゴメリリダクション演算の処理シーケンスを制御することにより、それぞれの処理における演算部の繰り返し回数が削減できる。

【図面の簡単な説明】

【図１】

本発明の一実施形態における多倍長演算装置の構成例を示す図

【図２】

本発明の一実施形態である加算剰余演算における演算部の構成例を示す図

【図３】

本発明の一実施形態である加算剰余演算におけるメモリ部のマップを示す図

【図４】

本発明の一実施形態である加算剰余演算における処理フローチャート

【図５】

本発明の一実施形態であるモンゴメリリダクションにおける演算部の構成例を示す図

【図６】

本発明の一実施形態であるモンゴメリリダクションにおけるstep1の処理を説明した図

【図７】

本発明の一実施形態であるモンゴメリリダクションにおけるstep2の処理を説明した図

【符号の説明】

１　演算部

２　メモリ部

３　サブメモリ１

４　サブメモリ２

５　メモリ入出力部

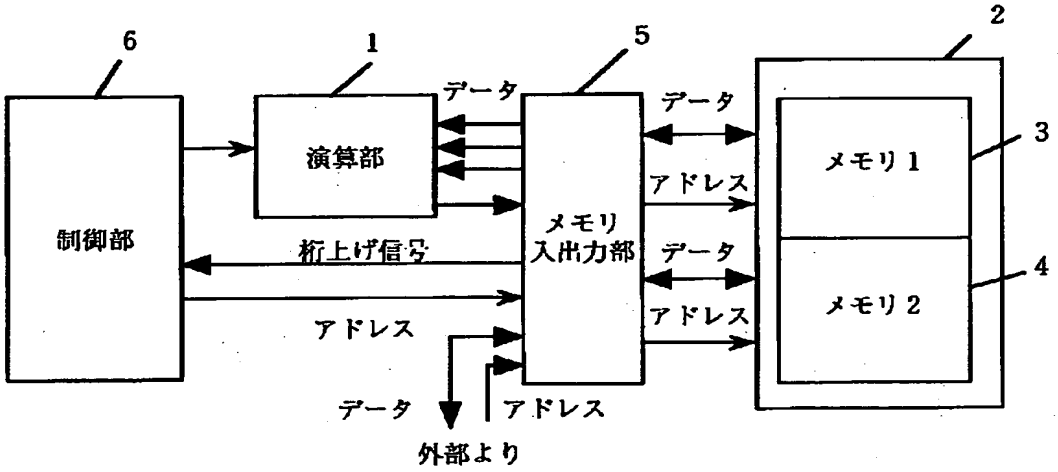
６　制御部

１０　３入力加算器

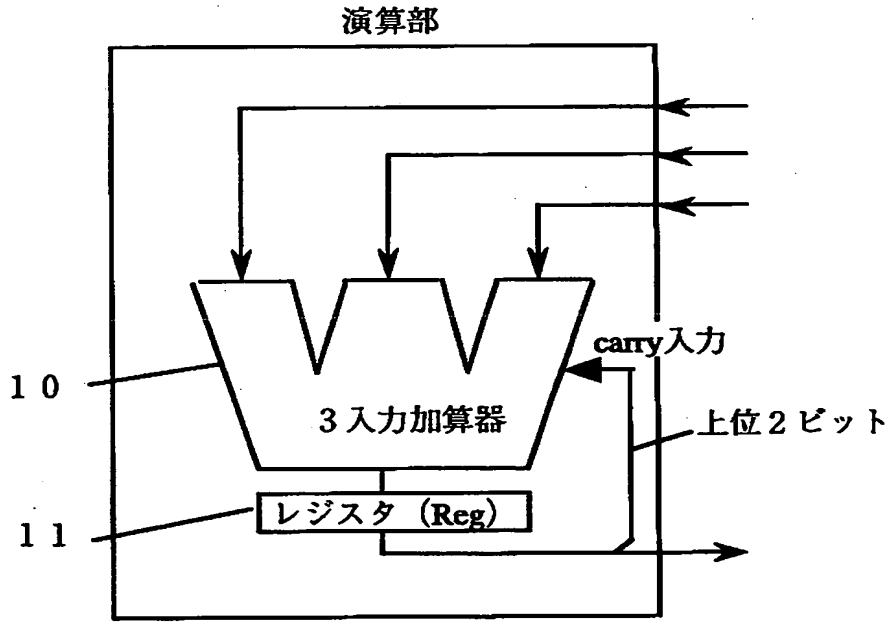
１１　レジスタ

【書類名】　　図面

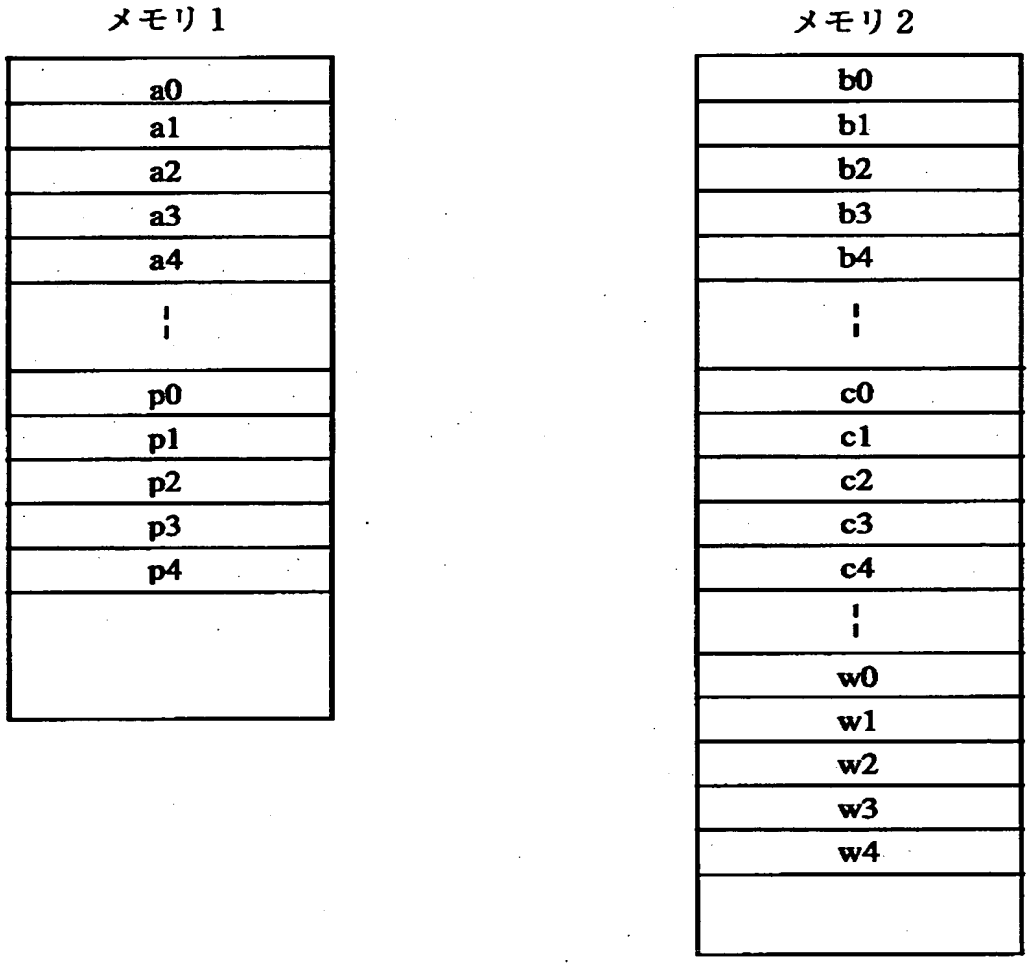
【図１】


6
1
5
2
データ
データ
演算部
メモリ１
3
制御部
アドレス
メモリ
入出力部
データ
4
桁上げ信号
メモリ２
アドレス
アドレス
データ
アドレス
外部より

【図２】

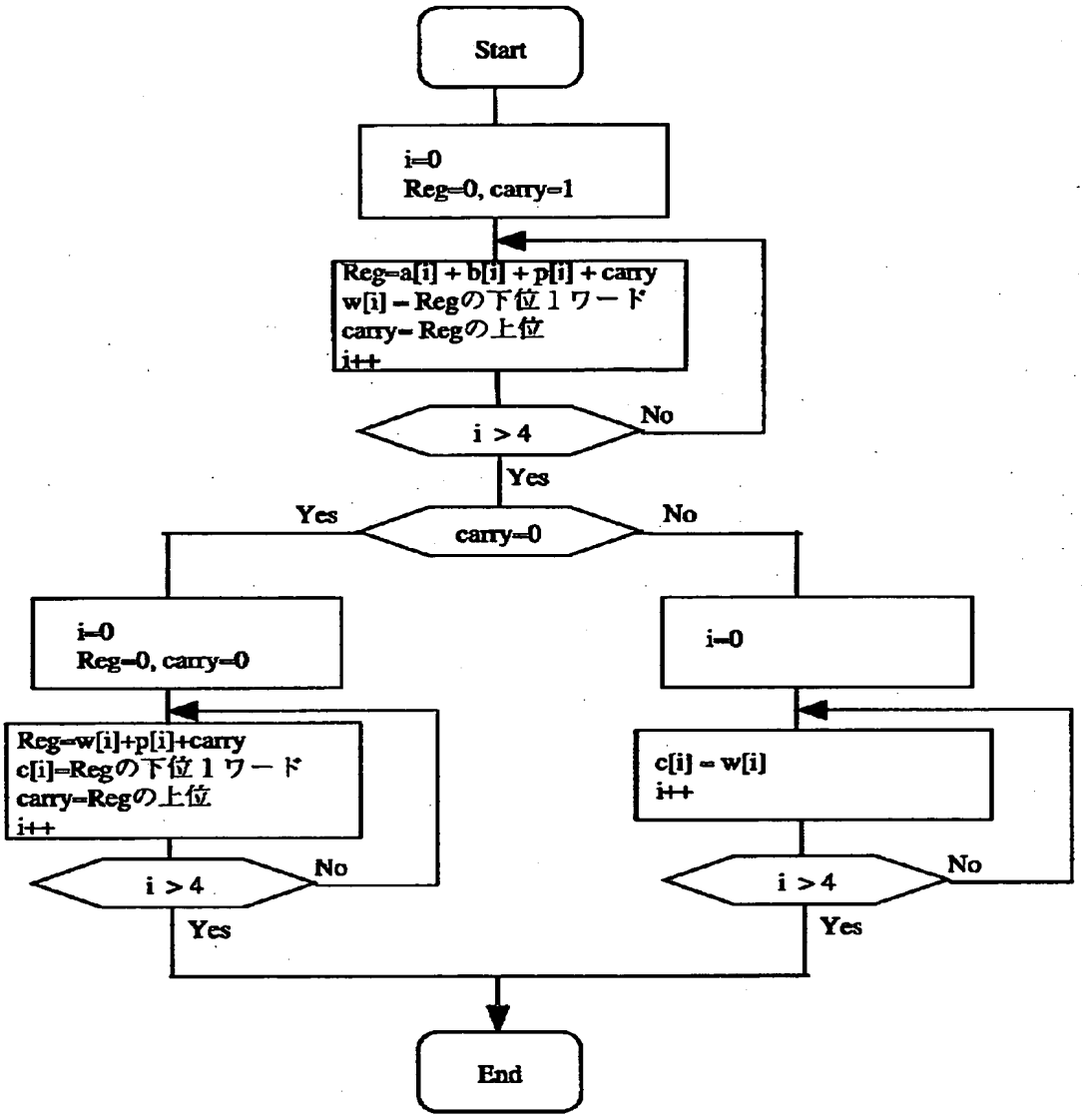

演算部
carry入力
１０
３入力加算器
上位２ビット
レジスタ（Reg）
１１

【図３】

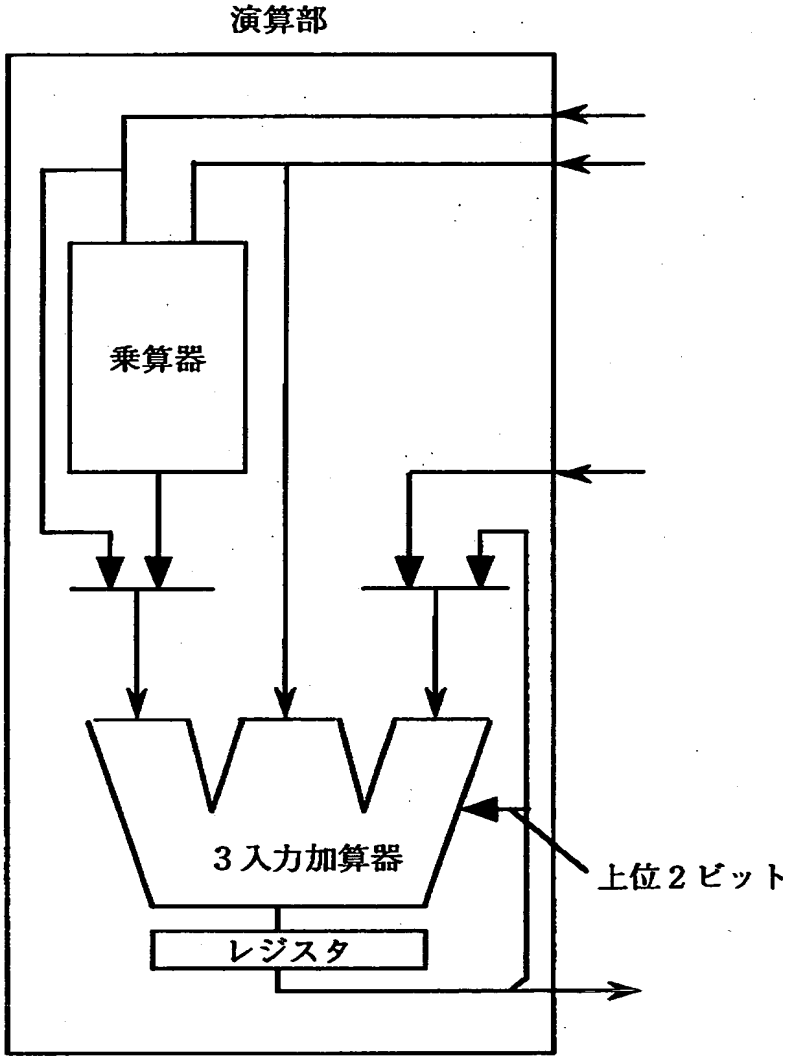


出証特２０００－３０２２９７４

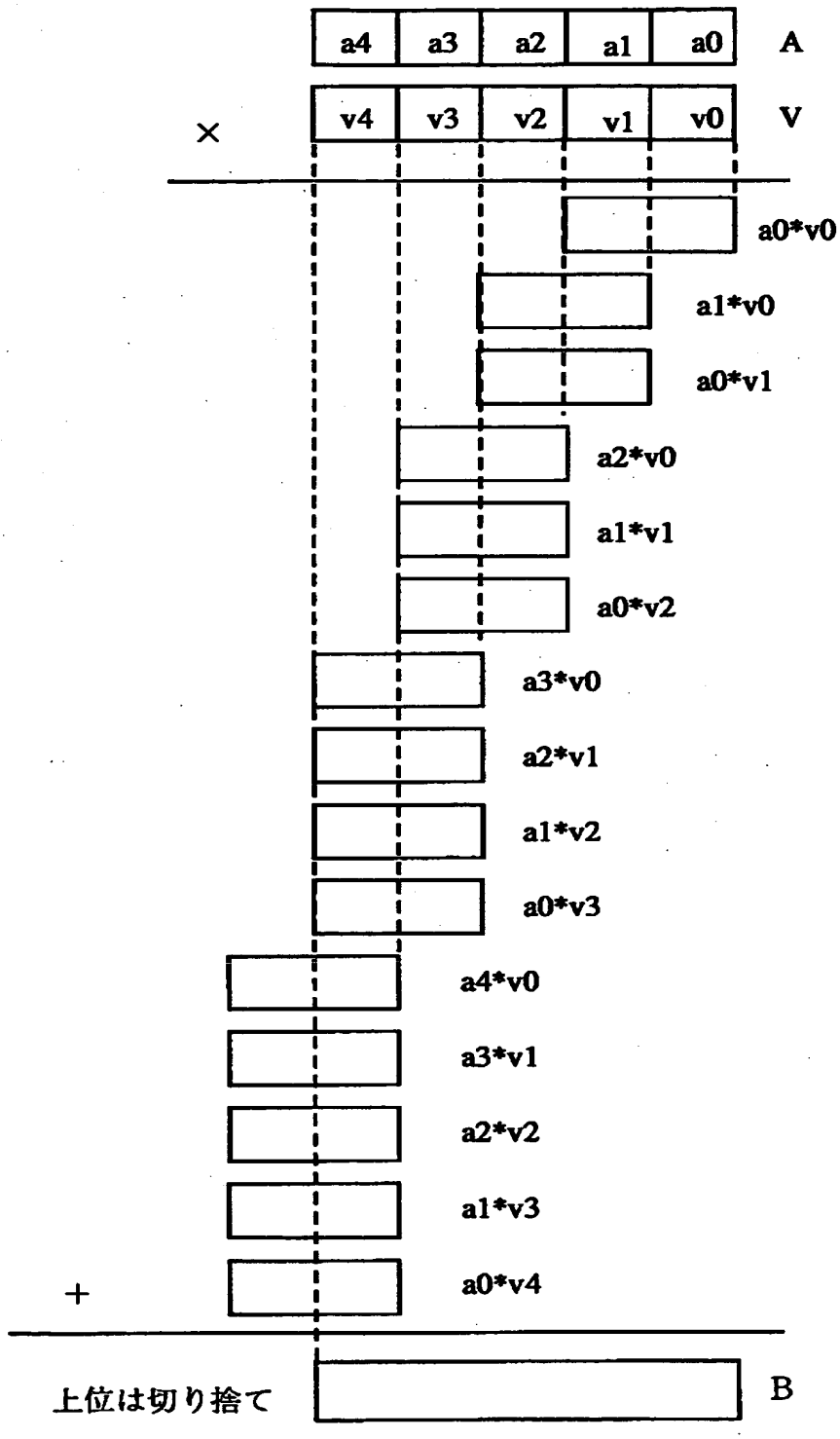
【図４】


Start
i=0
Reg=0, carry=1
Reg=a[i] + b[i] + p[i] + carry
w[i] = Regの下位１ワード
carry= Regの上位
i++
i > 4
No
Yes
carry=0
Yes
No
i=0
Reg=0, carry=0
Reg=w[i]+p[i]+carry
c[i]=Regの下位１ワード
carry=Regの上位
i++
i > 4
No
Yes
i=0
c[i] = w[i]
i++
i > 4
No
Yes
End

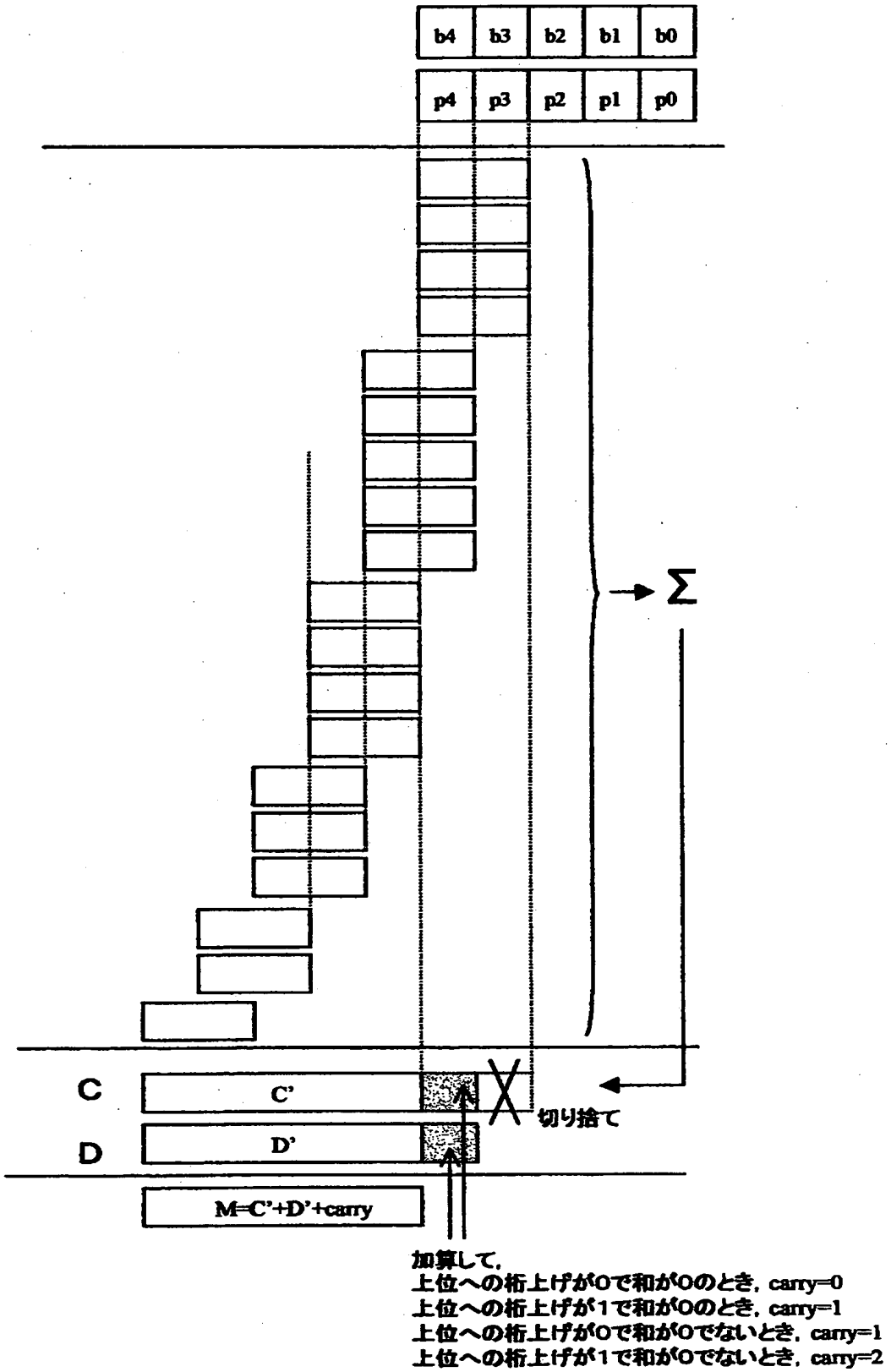
【図５】



【図６】


a4
a3
a2
a1
a0
A
×
v4
v3
v2
v1
v0
V
a0*v0
a1*v0
a0*v1
a2*v0
a1*v1
a0*v2
a3*v0
a2*v1
a1*v2
a0*v3
a4*v0
a3*v1
a2*v2
a1*v3
a0*v4
+
上位は切り捨て
B

【図７】


b4
b3
b2
b1
b0
p4
p3
p2
p1
p0
Σ
C
C'
切り捨て
D
D'
M=C'+D'+carry
加算して,
上位への桁上げが0で和が0のとき, carry=0
上位への桁上げが1で和が0のとき, carry=1
上位への桁上げが0で和が0でないとき, carry=1
上位への桁上げが1で和が0でないとき, carry=2

【書類名】　要約書

【要約】

【課題】　楕円演算のような複雑な演算を、小さなハードウェアで高速に実現する。制御を加えることにより楕円演算とRSA暗号演算が切り替えて実現できる。

【解決手段】　演算部とメモリ部と制御部からなる。演算部に効率的にデータを供給するメモリ部の構成とその制御方法が発明のポイント。加算剰余演算（A+B modP）では、演算部は3入力加算器からなり、入力A、B、法Ｐを同時に入力して、A+B-Pの計算を行う。この桁上げ信号により制御シーケンスを変更し、結果が負となる場合には、Pを加算して、最終的にA+B modPを求める。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社